MAXIMAL GALOIS GROUP OF
L-FUNCTIONS OF ELLIPTIC CURVES

F. JOUVE

ABSTRACT. We give a quantitative version of a result due to N. Katz about L-functions of elliptic curves over function fields over finite fields. Roughly speaking, Katz's Theorem states that, on average over a suitably chosen algebraic family, the L-function of an elliptic curve over a function field becomes "as irreducible as possible" when seen as a polynomial with rational coefficients, as the cardinality of the field of constants grows. A quantitative refinement is obtained as a corollary of our main result which gives an estimate for the proportion of elliptic curves studied whose L-functions have "maximal" Galois group . To do so we make use of E. Kowalski's idea to apply large sieve methods in algebro-geometric contexts. Besides large sieve techniques, we use results of C. Hall on finite orthogonal monodromy and previous work of the author on orthogonal groups over finite fields.

INTRODUCTION

In [Ka], Katz studies the irreducibility of the L-function of an elliptic curve over a function field in one variable over $\mathbf{F}_q$, when varying the curve among the elements of an algebraic family. A very down-to-earth instance of Katz's result goes as follows (see [Ka, Section 2]): let $Twist_d$ be the subspace of $\mathbf{A}^d_{\mathbf{F}_q}$ (where q is still assumed to be odd) consisting of monic polynomials of degree $d \geqslant 3$ for which $f(0)f(1)\mathrm{disc}(f)$ is invertible. For an $\mathbf{F}_q$-rational point $f \in Twist_d(\mathbf{F}_q)$, we consider the affine curve U which is the complement in $\mathbf{A}^1_{\mathbf{F}_q}$ of $0, 1$ and the zeros of f. We have the family of twisted Legendre elliptic curves (E_f) over U with affine part:

$$y^2 = f(\lambda)x(x-1)(x-\lambda).$$

From a fundamental Theorem of Grothendieck we know that the L-function $L(E_f/\mathbf{F}_q(t); T)$ attached to $E_f/\mathbf{F}_q(t)$ is a polynomial in T with coefficients in $\mathbf{Z}$. In the above setting, Katz's result asserts that as q grows the proportion of f in $Twist_d(\mathbf{F}_q)$ such that the reduced L-function of E_f (which is the quotient of $L(E_f/\mathbf{F}_q(t); T)$ by "trivial factors" we will make precise in Section 1) is a $\mathbf{Q}$-irreducible polynomial, tends to 1. That kind of question, of course, is linked to the function field version of the Birch-Swinnerton-Dyer conjecture. Indeed getting information on the irreducibility of the L-function of a given elliptic curve over $\mathbf{F}_q(t)$ tells us, a fortiori, about the order of vanishing of that function at 1.

In this paper we give a quantitative refinement of Katz's result. There are essentially two types of ingredients that come into play in our proof. First, for an odd prime ℓ invertible in the base field, the ℓ-torsion of the elliptic curves we consider gives rise to a family of $\mathbf{F}_\ell$-sheaves, the monodromy of which is controlled by results of C. Hall [Hall]. From loc. cit., we know that the finite monodromy groups arising are big subgroups of certain orthogonal groups and that imposes severe restrictions on the representation theory of those groups. The second main feature of our work consists in local computations for sets of matrices or polynomials over finite fields. Here we make a crucial use of results of [J]. In both cases one of the main issues comes from the lack of good topological properties of the orthogonal group (seen as an algebraic group over the rationals). As a matter of comparison, Kowalski in [KoZeta] establishes a similar quantitative refinement for a result of Chavdarov (see [Chav]). However these authors work in an algebro-geometric framework where $\mathbf{F}_\ell$-sheaves with symplectic monodromy naturally arise.

Therefore most of the main arguments used by Kowalski in [KoZeta] or Chavdarov in [Chav] cannot be applied or even adapted to our case because orthogonal groups do not share some nice properties that hold for the symplectic group ($\mathbf{O}(N)$ is not connected ans $\mathbf{SO}(N)$ is not simply connected).

Our last task is then to put things together in a large sieve framework we will make precise.

The paper is divided in the following sections: first, following [Hall], we give the precise context and recall the results we need to state a sample of our main Theorem. In Section 2 we set up the large sieve framework that enables us to gather our different pieces of data. In that section we state a large sieve inequality which is a crucial tool to obtain the kind of quantitative information we want. Finally in Section 3, we recall and make a few results from [J] more precise, so that putting things together yields a proof of our main result. We conclude by discussing uniformity issues in our result and we give a uniform estimate (in a sense we will make precise) in the case where E is a Legendre curve.

Notation. As usual the cardinality of a finite set X will be denoted $|X|$. If G is a group and S is a conjugacy invariant subset of G, we will denote by $S^\sharp$ the set of conjugacy classes of elements of S under G. If G is an abelian group, $\hat{G}$ will denote its group of characters.

The biggest integer smaller than a real number x will be denoted $\lfloor x \rfloor$. If p is a prime number and n is an integer, $v_p(n)$ will denote the p-adic valuation of n. Similarly, if $m(t)$ (resp. $P(t)$) is a polynomial (resp. an irreducible polynomial) in $k[t]$ (for some field k) then we will denote by $\mathrm{ord}_P(m)$ the exponent of $P(t)$ appearing in the decomposition of $m(t)$ as a product of irreducible polynomials.

We will make use of the Vinogradov notation $f \ll g$ or of the Landau notation $f = O(g)$ when there exists a strictly positive constant C such that $|f(x)| \leqslant Cg(x)$ for any x in a common subset of the domains of the functions f and g. If $\mathcal{P}_\kappa(S)$ is a property that a set S may satisfy depending on the value taken by a real parameter κ, we will write "$\mathcal{P}_\kappa(S)$ holds for $\kappa \geqslant \kappa_0(S)$" if the property $\mathcal{P}_\kappa(S)$ is true for a large enough value of κ that depends only on the choice of S.

For two n-tuples $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$ we will use the Kronecker symbol

$$\delta\big((x_1, \ldots, x_n), (y_1, \ldots, y_n)\big),$$

which equals 1 if $x_i = y_i$ for all $1 \leqslant i \leqslant n$ and 0 otherwise.

Finally we will denote by $\mathrm{disc}(f)$ the discriminant of a polynomial f (in the sense of e.g. [LaA, p. 204]) and by $\mathrm{disc}(Q)$ the discriminant of a quadratic form Q (i.e. the determinant of a Gram matrix for Q).

1. A QUANTITATIVE VERSION OF KATZ'S THEOREM

For q a fixed power of a fixed odd prime number p, let $E/\mathbf{F}_q(t)$ be an elliptic curve over the rational function field $K = \mathbf{F}_q(t)$ with non constant j-invariant. The L-function of E/K is well-known to be equal to a reversed characteristic polynomial in the variable T:

$$\det(1 - qTA),$$

where $A \in O(N, \mathbf{R})$, the orthogonal group for a real quadratic space of dimension N. As mentioned in the introduction we know that such a polynomial has integral coefficients. Following Katz (see [Ka]), we prefer studying the *unitarized* L-function of E/K:

$$L_u(E/K; T) = L(E/K; T/q) = \det(1 - TA),$$

which is a polynomial with coefficients in $\mathbf{Z}[1/q]$.

The question of the irreducibility of $L_u(E/K; T)$ seen as a $\mathbf{Q}$-polynomial is only relevant if there is no a priori imposed root for that polynomial. But, as $L_u(E/K; T)$ coincides with the

(reversed) characteristic polynomial of an orthogonal matrix A with size $N \times N$, it satisfies the well known functional equation

$$\det(1 - TA) = T^N \det(-A) \det(1 - T^{-1}A) \,. \tag{1}$$

As a consequence we will study the irreducibility (or indeed the maximality of the Galois group) of what Katz calls the *reduced L*-function:

(2)

$$L_{\mathrm{red}}(E/K; T) = \det(1 - TA)_{\mathrm{red}} = \begin{cases} \det(1 - TA)/(1 - \det(A)T) \,, \text{ if } N \text{ is odd}\,, \\ \det(1 - TA)/(1 - T^2) \,, \text{ if } N \text{ is even and } \det(A) = -1 \,, \\ \det(1 - TA) \,, \text{ otherwise}\,. \end{cases}$$

1.1. Quadratic twists and a particular cohomology space.

Notice that instead of the above piece of data $E/\mathbf{F}_q(t)$, we can suppose equivalently that we are given an elliptic fibration

$$\mathcal{E} \longrightarrow \mathbb{P}^1 \,.$$

Let $f \in K^\times/(K^\times)^2$ (i.e. we fix a class of $K^\times$ modulo the nonzero squares of K). We denote by E_f the quadratic twist of E by f: this is the elliptic curve such that $E_f \simeq E$ over a quadratic extension of K but not over K itself. For each such f we have an elliptic pencil

$$\mathcal{E}_f \longrightarrow \mathbb{P}^1 \,.$$

The group of sections $\mathcal{E}_f(\mathbb{P}^1)$ for that fibration can be identified with the Mordell-Weil group $E_f(K)$ and the multiplication by ℓ morphism

$$E_f(K) \xrightarrow{\times \ell} E_f(K) \,,$$

gives rise, for each ℓ invertible in $\mathbf{F}_q$, to the isogeny of group schemes

$$\mathcal{E}_f^{\mathrm{lisse}} \xrightarrow{\times \ell} \mathcal{E}_f^{\mathrm{lisse}} \,,$$

where $\mathcal{E}_f^{\mathrm{lisse}}$ is the smooth part of the Néron model $\mathcal{E}_f \longrightarrow \mathbb{P}^1$ of E/K. The kernel $\mathcal{E}_{f,\ell}$ of that last arrow is an étale group scheme over $\mathbb{P}^1$ and the fiber of $\mathcal{E}_{f,\ell}$ over a geometric generic point of $\mathbb{P}^1$ is $E_f[\ell]$, the ℓ-torsion of $E_f(K)$ (it might only be a subspace of it though, if we do not assume the geometric point we consider to be generic).

Now let $\mathcal{V}_{f,\ell}$ denote the étale cohomology group $H^1(\mathbb{P}^1 \times \overline{\mathbf{F}_q}, \mathcal{E}_{f,\ell})$. There is an additional quadratic structure on $\mathcal{V}_{f,\ell}$. Indeed the usual Weil pairing on $E_f[\ell] \times E_f[\ell]$ extends to a non-degenerate alternating pairing

$$\mathcal{E}_{f,\ell} \times \mathcal{E}_{f,\ell} \longrightarrow \mathbf{F}_\ell(1) \,,$$

where $\mathbf{F}_\ell(1)$ denotes the usual Tate twist. Poincaré duality yields a non degenerate symmetric pairing

$$\mathcal{V}_{f,\ell} \times \mathcal{V}_{f,\ell} \longrightarrow H^2(\mathbb{P}^1 \times \overline{\mathbf{F}_q}, \mathbf{F}_\ell(1)) \,.$$

That last cohomology space being isomorphic to $\mathbf{F}_\ell$, we end up with a non-degenerate symmetric bilinear form on $\mathcal{V}_{f,\ell}$ for which the endomorphism Fr_q (induced on $\mathcal{V}_{f,\ell}$ by the global Frobenius on $\mathbb{P}^1$) is a conjugacy class of isometries (i.e. of elements of the associated orthogonal group $O(\mathcal{V}_{f,\ell})$).

1.2. A 1-parameter family of quadratic twists.

With notation as above, we work under the assumptions of [Hall, Section 6.2]: we suppose that $\mathcal{E} \longrightarrow \mathbb{P}^1$ has at least one fiber of multiplicative reduction away from ∞ and we fix a nonzero polynomial $m \in \mathbf{F}_q[t]$ which vanishes at (at least) one point of the locus of multiplicative reduction so that, for any f, the fibration $\mathcal{E}_f \longrightarrow \mathbb{P}^1$ also has at least one fiber of multiplicative reduction away from ∞. Now consider for every integer $d \geqslant 1$

$$F_d = \{ f \in \overline{\mathbf{F}_q}[t] \mid f \text{ is squarefree}, \deg(f) = d, \gcd(f, m) = 1 \} \,.$$

A remarkable property that F_d satisfies is that the degree of the L-function of the twisted curve $E_f/\mathbf{F}_{q^n}$ does neither depend on the choice of $f \in F_d(\mathbf{F}_{q^n})$ nor on n but only on d (see [Hall,

beginning of 6.2]). The degree N of $L(E_f/\mathbf{F}_{q^n}(t); T)$ is explicitly given in Lemma 6.2 of loc. cit. by

(3)
$$N = \deg(M_f) + 2\deg(A_f) - 4,$$

where M_f (resp. A_f) is the divisor of multiplicative (resp. additive) reduction of $\mathcal{E}_f \longrightarrow \mathbb{P}^1$.

Instead of considering the whole variety F_d, we restrict ourselves to a one parameter subfamily of polynomials in F_d. The reason for such a restriction will become clear when we get into the details of the estimates we want to establish. The corresponfing curve is the following open subset of $\mathbf{A}^1$:
$$U_g = \{c \in \mathbf{A}^1(\overline{\mathbf{F}_q}) \mid (c-t)g(t) \in F_d\}$$
where g is a fixed element of F_{d-1}. The geometric points of U_g can easily be seen as the complementary in $\mathbf{A}^1(\overline{\mathbf{F}_q})$ of the union of the set of roots of g and m. Finally, for $c \in U_g(\mathbf{F}_q)$ let us denote by E_c the quadratic twist of E by the $\mathbf{F}_q$-polynomial $(c-t)g(t) \in F_d(\mathbf{F}_q)$. We can state a sample of our main result as follows:

Theorem 1. *With notation as above, let $L_{\mathrm{red},c}$ denote the reduced L-function of the quadratic twist E_c of E . For $N \geqslant 5$, $d = \deg(g) + 1 \geqslant d_0(E)$, and $q \geqslant q_0(E)$, we have*

$$|\{c \in \mathbf{A}^1(\mathbf{F}_q) \mid g(c) \neq 0, m(c) \neq 0 \text{ and } L_{\mathrm{red},c} \text{ is reducible }\}| \ll q^{1-\gamma} \log q,$$

where the implied constant depends only on E and where we can choose $2\gamma^{-1} = 7N^2 - 7N + 4$.

2. A LARGE SIEVE INEQUALITY

In this section, we describe the large sieve framework thanks to which we will finally obtain quantitative estimates such as the one stated in Theorem 1. The idea of using sieve methods in algebro-geometric contexts was first introduced by Kowalski in [KoZeta] to study the irreducibility and the maximality of the Galois group of numerators of zeta functions of certain curves over finite fields (see [KoSieve, Chap. 8] for a general discussion on the subject and [KoZeta2] for an application to algebraic independence of the zeros of the numerators of those zeta functions).

2.1. **The geometric setting.** To begin with, let us fix a parameter variety $U/\mathbf{F}_q$. We assume it to be smooth, affine and geometrically connected with dimension $d \geqslant 1$. If $\bar{U}$ denotes the extension of scalars $U \times \overline{\mathbf{F}_q}$ to a separable closure of $\mathbf{F}_q$ and $\bar{\eta}$ is a fixed geometric point on U, we may denote by $\pi_1(U, \bar{\eta})$ (resp. $\pi_1(\bar{U}, \bar{\eta})$) the étale arithmetic (resp. geometric) fundamental group of $U/\mathbf{F}_q$. These groups fit the exact sequence

(4)
$$1 \longrightarrow \pi_1(\bar{U}, \bar{\eta}) \longrightarrow \pi_1(U, \bar{\eta}) \xrightarrow{\deg} \hat{\mathbf{Z}} \longrightarrow 1,$$

where $\hat{\mathbf{Z}}$ stands for the profinite completion of $\mathbf{Z}$ and the degree map deg is such that $\deg(\mathrm{Fr}_u) = -n$ if Fr_u denotes the local geometric Frobenius at $u \in U(\mathbf{F}_{q^n})$, for any $n \geqslant 1$.

The next piece of data is, for ℓ running over a fixed set of primes Λ (that will be specified in the application we have in mind), a family of sheaves $(\mathcal{F}_\ell)_\ell$ of $\mathbf{F}_\lambda$-vector spaces on U (where $\mathbf{F}_\lambda$ is, for each ℓ, a fixed finite extension of $\mathbf{F}_\ell$) with rank $N \geqslant 1$. Equivalently, for each $\ell \in \Lambda$, we are given a continuous representation

$$\rho_\ell : \pi_1(U, \bar{\eta}) \longrightarrow GL(N, \mathbf{F}_\lambda).$$

The *arithmetic $\mathbf{F}_\ell$-monodromy group* G_ℓ associated to that representation is defined as its image whereas the *geometric $\mathbf{F}_\ell$-monodromy group* attached to ρ_ℓ is the image G_ℓ^g of the subgroup $\pi_1(\bar{U}, \bar{\eta})$. Unlike the case treated in [KoZeta] where the monodromy groups involved are symplectic groups, we will have to deal with orthogonal monodromy groups in our applications. So we suppose that, for each ℓ, we have an inclusion $G_\ell \subset O(N, \mathbf{F}_\ell)$ into the orthogonal group for some $\mathbf{F}_\ell$-quadratic space of dimension N.

Finally we put the emphasis on the first major difference with the case of a geometric setting involving symplectic monodromy: we need to suppose we are given an étale Galois cover

$$\kappa : V \longrightarrow U,$$

with abelian Galois group $G(V/U)$ which we assume to be an elementary 2-group. If $\bar{\mu}$ denotes a geometric point on V such that $\kappa \circ \bar{\mu} = \bar{\eta}$, then, by functoriality, we know these groups fit the exact sequence

$$1 \longrightarrow \pi_1(V, \bar{\mu}) \xrightarrow{\pi_1\kappa} \pi_1(U, \bar{\eta}) \xrightarrow{\tilde{\varphi}} G(V/U) \longrightarrow 1\,,$$

where the quotient morphism $\tilde{\varphi}$ is induced by the map

$$\varphi : U(\mathbf{F}_q) \longrightarrow G(V/U)$$

such that the image of $x \in U(\mathbf{F}_q)$ "is" the action of $\pi_1(U, \bar{\eta})$ on $\kappa^{-1}\{x\}$.

For each $\ell \in \Lambda$, the sheaf $\mathcal{F}_\ell$ can be pulled back to a lisse $\mathbf{F}_\ell$-adic sheaf $\kappa^*\mathcal{F}_\ell$ on V. Our crucial assumption is that the sheaf obtained has big geometric $\mathbf{F}_\ell$-monodromy in the sense of Hall (see [Hall]), for every $\ell \in \Lambda$ i.e.

$$G_\ell^{g,V} = \rho_\ell(\pi_1(\bar{V}, \bar{\mu})) \supset \Omega(N, \mathbf{F}_\ell)\,,$$

where we omit to write the inclusion $\pi_1\kappa$ for brevity and where $\Omega(N, \mathbf{F}_\ell)$ stands for the derived group of $O(N, \mathbf{F}_\ell)$.

Moreover we assume that the family $(\kappa^*\mathcal{F}_\ell)_\ell$ is *linearly disjoint* in the sense that, for every $\ell \neq \ell' \in \Lambda$, the product map

$$\rho_{\ell,\ell'} = \rho_\ell \times \rho_{\ell'} : \pi_1(U, \bar{\eta}) \longrightarrow G_\ell \times G_{\ell'}$$

satisfies

$$\rho_{\ell,\ell'}(\pi_1(\bar{V}, \bar{\mu})) = G_{\ell,\ell'}^{g,V} = G_\ell^{g,V} \times G_{\ell'}^{g,V} \supset \Omega(N, \ell) \times \Omega(N, \ell')\,.$$

In order to unify the notation, the morphism $\rho_{\ell,\ell'}$ (resp. the group $G_{\ell,\ell'}^{g,V}$) will simply denote ρ_ℓ (resp. $G_\ell^{g,V}$) in the case $\ell = \ell'$.

Now we obtain for each $\ell \in \Lambda$ the following diagram with exact rows and surjective downward arrows, by putting the above data together with (4):

(5)
$$\begin{array}{ccccccccc}
1 & \longrightarrow & \pi_1(\bar{V}, \bar{\mu}) & \longrightarrow & \pi_1(U, \bar{\eta}) & \xrightarrow{(\deg, \tilde{\varphi})} & \Gamma & \longrightarrow & 1 \\
& & \downarrow{\scriptstyle \rho_\ell} & & \downarrow{\scriptstyle \rho_\ell} & & \downarrow{\scriptstyle \mathrm{pr}_\ell} & & \\
1 & \longrightarrow & G_\ell^{g,V} & \longrightarrow & G_\ell & \xrightarrow{(\deg, \tilde{\varphi}_\ell)} & \Gamma_\ell & \longrightarrow & 1\,,
\end{array}$$

where pr_ℓ is defined in such a way that the diagram commutes, and, in the bottom row, deg stands for the quotient morphism $G_\ell \longrightarrow G_\ell/G_\ell^g$, with $G_\ell^g = \rho_\ell(\pi_1(\bar{U}, \bar{\eta}))$.

A few comments are in order here: first, (5) is the analogue of the diagram (2.2) in [KoZeta]. Next, the quotient group $\Gamma \leqslant \hat{\mathbf{Z}} \times G(V/U)$ is abelian and the quotient group Γ_ℓ is a subgroup of the Kleinian group $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Indeed the subgroup $\Omega(N, \mathbf{F}_\ell)$ is normal with index four in $O(N, \mathbf{F}_\ell)$ and the associated quotient is $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ (see [Ka, Section 6] or [J, Section 2]). The fact that, contrary to [KoZeta], we need to introduce the auxiliary variety V is because of the assumption of linear disjointness. Indeed, as noticed in loc. cit., there are proper subgroups of $O(N, \mathbf{F}_\ell) \times O(N, \mathbf{F}_{\ell'})$ which project surjectively on both factors, e.g.

$$H_{\ell,\ell'} = \{(g, g') \mid \det(g) = \det(g')\}\,,$$

where the equality of determinants is seen in $\{\pm 1\}$. As a consequence, if ever, in the applications, we come up with a family of sheaves $(\mathcal{F}_\ell)_\ell$ on U with geometric monodromy as big as $O(N, \mathbf{F}_\ell)$, then we cannot hope for linear disjointness for $(\mathcal{F}_\ell)_\ell$ itself. We emphasize here that such precautions need not be taken in the case (studied in [KoZeta]) of a family of sheaves with symplectic $\mathbf{F}_\ell$-monodromy.

2.2. **Sieving for Frobenius.** Thanks to the data contained in (5), we can perfrom a "coset sieve" as described in a very general context in [KoSieve, Chap. 3] with complements that can be found in [J]. In our case the finite set which is to be sifted is given, for a fixed $\alpha \in G(V/U)$, by

$$X_\alpha = \{u \in U(\mathbf{F}_q) \mid \varphi(u) = \tilde{\varphi}(\mathrm{Fr}_u) = \alpha\}.$$

Note, that a particular feature of our study is that two left cosets are considered simultaneously: on the one hand we restrict to local Frobenii with degree -1 (i.e. to $\mathbf{F}_q$-rational points on U) and on the other hand, among the remaining Frobenii, we only keep those mapping to α under $\tilde{\varphi}$.

Then we define Y to be "the set X_α seen on the fundamental group level":

$$Y = \{g^\sharp \in \pi_1(U, \bar{\eta})^\sharp \mid \tilde{\varphi}(g^\sharp) = \alpha \ \text{ and } \ \deg(g^\sharp) = -1\},$$

where $g^\sharp$ denotes the conjugacy class of g.

For each $\ell \in \Lambda$, we can then define $Y_\ell = \rho_\ell(Y)$ so that if we set $\alpha_\ell = \mathrm{pr}_\ell(-1, \alpha)$, then Y_ℓ is the left coset for which α_ℓ is a representative. Now let $L \geqslant 1$ be a fixed integer and let $\Theta = (\Theta_\ell)_\ell$ be a family of conjugacy invariant subsets $\Theta_\ell \subset Y_\ell$. In this section, our purpose is to give an upper bound for the cardinality of the set

$$S(X_\alpha, \Theta, L) = \{u \in X_\alpha \mid \rho_\ell(\mathrm{Fr}_u) \notin \Theta_\ell \text{ for all } \ell \in \Lambda, \ell \leqslant L\}.$$

Note that, alternatively, we could define Λ as a subset of the prime numbers smaller than a fixed $L \geqslant 1$. This is in fact what we will do in the proof of Theorem 10.

Let Π_ℓ denote a set of representatives (containing 1) for the equivalence classes of irreducible representations of G_ℓ identifying two irreducible representations π and τ if and only if their restrictions to $G_\ell^{g,V}$ coincide. If Π_ℓ^* denotes the subset of $\Pi_\ell \setminus \{1\}$ consisting of representations π whose character restricted to Y_ℓ does not identically vanish, then we have the following inequality (a proof of which can be found, in a more general context, in [KoSieve, Chap. 3])

(6) $$|S(X_\alpha, \Theta, L)| \leqslant \Delta H^{-1},$$

where

$$H = \sum_{\ell \leqslant L} \left(|\Theta_\ell| (|G_\ell^{g,V}| - |\Theta_\ell|)^{-1} \right),$$

and

$$\Delta \leqslant \max_{\ell \leqslant L} \max_{\ell \in \Pi_\ell^*} \sum_{\ell' \leqslant L} \sum_{\tau \in \Pi_{\ell'}^*} |W(\pi, \tau)|,$$

where $W(\pi, \tau)$ is an "exponential sum" given by

(7) $$W(\pi, \tau) = \frac{1}{\sqrt{|\hat{\Gamma}_\ell^\pi||\hat{\Gamma}_{\ell'}^\tau|}} \sum_{u \in X_\alpha} \mathrm{Tr}\big(\pi \rho_\ell(\mathrm{Fr}_u)\big) \overline{\mathrm{Tr}\big(\tau \rho_{\ell'}(\mathrm{Fr}_u)\big)},$$

and $\hat{\Gamma}_\ell^\pi = \{\psi \text{ character of } G_\ell/G_\ell^{g,V} \mid \pi \simeq \pi \otimes \psi\}$.

The inequality (6) will be refered to as the large sieve inequality and Δ will be called the large sieve constant. Obviously, obtaining an efficient upper bound for $|S(X_\alpha, \Theta, L)|$ proceeds in two steps: first we need to find a good upper bound for Δ (this is the task this section is devoted to) and second we need to produce a lower bound for H (which is one of the goals of Section 3). As far as Δ is concerned, the above a priori bound involving the sums $W(\pi, \tau)$ suggests that we could try to estimate those sums individually and hope for as much cancellation as possible. In order to apply that strategy we need to make a few additional assumptions. If our base variety is a curve, that involves the notion of *compatible system of sheaves*:

Definition 2. With the same notation as above, a system of continuous representations $(\rho_\ell)_\ell : \pi_1(U, \bar{\eta}) \longrightarrow GL(r, k_\ell)$ (where k_ℓ is a finite extension of $\mathbf{F}_\ell$) indexed by a set of primes Λ not containing p, is said to be *compatible* if there exists a number field $\mathcal{K}/\mathbf{Q}$ and for each $\ell \in \Lambda$ a

prime ideal $\lambda \in \mathbf{Z}_\mathcal{K}$ (the ring of integers of $\mathcal{K}$) such that, on the one hand $\mathbf{Z}_\mathcal{K}/\lambda \simeq k_\ell$, and on the other hand there exists a continuous morphism

$$\tilde{\rho}_\ell : \pi_1(U, \bar{\eta}) \longrightarrow GL(r, \mathbf{Z}_\lambda),$$

(where $\mathbf{Z}_\lambda$ is the ring of integers of the completion $\mathcal{K}_\lambda$ of $\mathcal{K}$ with respect to λ) such that
- for each $\ell \in \Lambda$, the reduction $\tilde{\rho}_\ell$ modulo λ is isomorphic to ρ_ℓ,
- for each $\ell \in \Lambda$, each extension $\mathbf{F}_{q^n}/\mathbf{F}_q$ and each $u \in U(\mathbf{F}_{q^n})$, the reversed characteristic polynomial

$$\det(1 - T\tilde{\rho}_\ell(\mathrm{Fr}_u)) \in \mathbf{Z}_\lambda[T]$$

has coefficients in $\mathbf{Z}_\mathcal{K}$ and is independent of ℓ.

We can now state the key proposition, giving the expected cancellation for the sums $W(\pi, \tau)$ under certain condtions.

Proposition 3. *With the same notation as above, suppose $\pi \in \Pi_\ell^*$ and $\tau \in \Pi_{\ell'}^*$. Then the normalised exponential sums $W(\pi, \tau)$ satisfy:*

(1) *if $G_\ell^{g,V}$ has order prime to p for all $\ell \in \Lambda$, then*

$$W(\pi, \tau) = \delta((\ell, \pi), (\ell', \tau))\varepsilon_\pi q^d + O\Big(q^{d-1/2}|G_{\ell,\ell'}||G(V/U)|(\dim \pi)(\dim \tau)\Big)$$

where the implied constant depends only on $\bar{U}$.

(2) *if U is a curve (i.e. $d = 1$) and $(\mathcal{F}_\ell)_\ell$ forms a compatible system of sheaves (obtained as the reduction of a system $(\tilde{\mathcal{F}}_\ell)_\ell$ of $\mathbf{Z}_\ell$-adic sheaves), then*

$$W(\pi, \tau) = \delta((\ell, \pi), (\ell', \tau))\varepsilon_\pi q + O\Big(q^{1/2}(\dim \pi)(\dim \tau)\Big),$$

where the implied constant only depends on the compactly supported Euler-Poincaré characteristic of $\bar{U}$ and on the system $(\tilde{\mathcal{F}}_\ell)$ on $\bar{U}$.

Moreover, in both cases, the constant ε_π is uniformly bounded by 1 (i.e. $\varepsilon_\pi \leqslant 1$ independently of ℓ and π).

Proof. Forgetting for a while the normalisation factor in (7), we consider

$$W'(\pi, \tau) = \sum_{u \in X_\alpha} \mathrm{Tr}\big(\pi\rho_\ell(\mathrm{Fr}_u)\big)\overline{\mathrm{Tr}\big(\tau\rho_{\ell'}(\mathrm{Fr}_u)\big)}.$$

Using Frobenius reiprocity yields

$$W'(\pi, \tau) = \sum_{u \in U(\mathbf{F}_q)} \mathrm{Tr}\big(\pi\rho_\ell(\mathrm{Fr}_u)\big)\overline{\mathrm{Tr}\big(\tau\rho_{\ell'}(\mathrm{Fr}_u)\big)}\frac{1}{|G(V/U)|}\sum_{\chi \in \hat{G}(V/U)} \overline{\chi(\alpha)}\chi(\tilde{\varphi}(\mathrm{Fr}_u)),$$

so that we are naturally led to consider the sums

$$W_\chi(\pi, \tau) = \sum_{u \in U(\mathbf{F}_q)} \mathrm{Tr}\big(\pi\rho_\ell(\mathrm{Fr}_u)\big)\overline{\mathrm{Tr}\big(\tau\rho_{\ell'}(\mathrm{Fr}_u)\big)}\chi(\tilde{\varphi}(\mathrm{Fr}_u)),$$

for each character $\chi \in \hat{G}(V/U)$. The last two sums are thus related by the formula

$$W'(\pi, \tau) = \frac{1}{|G(V/U)|}\sum_{\chi \in \hat{G}(V/U)} \overline{\chi(\alpha)}W_\chi(\pi, \tau).$$

For a fixed χ, the sum $W_\chi(\pi, \tau)$ is closely related to the representation $\pi\rho_\ell \otimes \overline{\tau\rho_{\ell'}} \otimes \chi\tilde{\varphi}$ of the arithmetic fundamental group $\pi_1(U, \bar{\eta})$. To that representation corresponds an étale sheaf $\mathcal{F}_\chi(\pi, \tau)$, so that, applying the Grothendieck-Lefschetz trace formula (see [G]), we get

$$W_\chi(\pi, \tau) = \sum_{i=0}^{2d} (-1)^i \mathrm{Tr}(\mathrm{Fr} \mid H_c^i(\bar{U}, \mathcal{F}_\chi(\pi, \tau))),$$

where Fr denotes the morphism induced on the compactly supported étale cohomology by the global (geometric) Frobenius on $\bar{U}$.

The whole point of the proof is to give a precise analysis of that sum. First let us denote

$$[\pi, \bar{\tau}] = \begin{cases} \pi \boxtimes \bar{\tau} \text{ if } \ell \neq \ell', \\ \pi \otimes \bar{\tau} \text{ if } \ell = \ell', \end{cases}$$

where we distinguish the "external" tensor product "$\boxtimes$" from the "internal" tensor product "$\otimes$". Then, using the same notation as above, we have

$$\pi \rho_\ell \otimes \overline{\tau \rho_{\ell'}} = [\pi, \bar{\tau}] \rho_{\ell, \ell'} \, .$$

Using the additional notation $G_{\ell, \ell'} = \rho_{\ell, \ell'}(\pi_1(U, \bar{\eta}))$, we see that the representation $[\pi, \bar{\tau}] \rho_{\ell, \ell'} \otimes \chi \tilde{\varphi}$ corresponding to $\mathcal{F}_\chi(\pi, \tau)$, factors through a finite group:

$$\pi_1(U, \bar{\eta}) \overset{\rho_{\ell,\ell'} \times \tilde{\varphi}}{\longrightarrow} G_{\ell, \ell'} \times G(V/U) \overset{[\pi, \bar{\tau}] \boxtimes \chi}{\longrightarrow} GL((\dim \pi)(\dim \tau), \mathbf{C}) \, .$$

So any eigenvalue of any Fr_u, with $u \in U(\mathbf{F}_{q^n})$ acting on the fiber of $\mathcal{F}_\chi(\pi, \tau)$ at a geometric point $\bar{u}$ lying above u is a root of unity. In other words, $\mathcal{F}_\chi(\pi, \tau)$ is pointwise pure of weight 0. From a celebrated Theorem of Deligne [DeW, page 138], we deduce that the global geometric Frobenius Fr acts on each $H_c^i(\bar{U}, \mathcal{F}_\chi(\pi, \tau))$ with eigenvalues of modulus $\leqslant q^w$ for some integer $w \leqslant i/2$.

Now in the sum $W_\chi(\pi, \tau)$, the main contribution comes from the trace of Frobenius on the cohomology space with highest degree $H_c^{2d}(\bar{U}, \mathcal{F}_\chi(\pi, \tau))$. The above argument yields the following estimate for the sum of the other contributions:

Lemma 4. *We have the following estimates:*

(1) *if $G_{\ell, \ell'}$ has order prime to p, then*

$$\Big| \sum_{i=0}^{2d-1} (-1)^i \mathrm{Tr}(\mathrm{Fr} \mid H_c^i(\bar{U}, \mathcal{F}_\chi(\pi, \tau))) \Big| \leqslant q^{d-1/2} C(\bar{U}) |G_{\ell, \ell'}| |G(V/U)| (\dim \pi)(\dim \tau) \, ,$$

where $C(\bar{U})$ is a constant depending only on $\bar{U}$.

(2) *if $d = 1$ (i.e. U is a curve) and the family (ρ_ℓ) is obtained by reducing a compatible system of ℓ-adic sheaves, then*

$$\Big| \sum_{i=0}^{2d-1} (-1)^i \mathrm{Tr}(\mathrm{Fr} \mid H_c^i(\bar{U}, \mathcal{F}_\chi(\pi, \tau))) \Big| \leqslant q^{1/2} C(\bar{U}, (\rho_\ell))(\dim \pi)(\dim \tau) \, ,$$

where the constant $C(\bar{U}, (\rho_\ell))$ depends only on the compactly supported Euler-Poincaré characteristic of $\bar{U}$ and the compatible system.

Proof. This follows directly from the discussion preceding the statement of the lemma and [KoSieve, Prop. 8.9] (to which we refer for precise expressions for the constants $C(\bar{U})$ in case (1) and $C(\bar{U}, (\rho_\ell))$ in case (2)).

For instance, to derive (2) from loc. cit., we need only notice that (2) of [KoSieve, Prop. 8.9] holds for a representation ρ of the type $\rho_{\ell, \ell'} \times \tilde{\varphi}$ with values in $G_{\ell, \ell'} \times G(V/U)$ since $G(V/U)$ is assumed to be an elementary 2-group and thus can be seen as a subgroup of a product of type $\prod_i GL(1, k_i)$ where k_i is a finite field with characteristic $\ell_i \neq p$. $\square$

It remains now to determine precisely what the main contribution is. It is enough to determine the dimension of the cohomology space of degree $2d$ and then to show that the global geometric Frobenius acts with eigenvalues which are all equal and have for common value $\pm q^d$. Notice first that we have, from the Hochschild-Serre spectral sequence,

$$H_c^{2d}(\bar{U}, \mathcal{F}_\chi(\pi, \tau)) = H_c^{2d}(\bar{V}, \kappa^* \mathcal{F}_\chi(\pi, \tau))^{G^g(V/U)} \, ,$$

where the group $G^g(V/U)$ is the "geometric" version of the Galois group of the cover $\kappa : V \longrightarrow U$, i.e. it is defined via the exact sequence

$$1 \longrightarrow \pi_1(\bar{V}, \bar{\mu}) \longrightarrow \pi_1(\bar{U}, \bar{\eta}) \longrightarrow G^g(V/U) \longrightarrow 1 \, .$$

The cohomology space $H_c^{2d}(\bar{V}, \kappa^* \mathcal{F}_\chi(\pi, \tau))$ coincides with the space of coinvariants (see [De, Sommes trig., Rem. 1.18d])

$$\left(\pi \rho_\ell \otimes \overline{\tau \rho_{\ell'}} \otimes \chi \tilde{\varphi} \right)_{\pi_1(\bar{V}, \bar{\mu})}(-d) \,,$$

which is the d-th Tate twist of the space of coinvariants of the representation $\pi \rho_\ell \otimes \overline{\tau \rho_{\ell'}} \otimes \chi \tilde{\varphi}$ seen as a $\pi_1(\bar{V}, \bar{\mu})$-module. First, we focus on dimension issues. In the last part of the proof we will show that Frobenius acts as $\pm \mathrm{Id}$ on the space of coinvariants $H_c^{2d}(\bar{U}, \mathcal{F}_\chi(\pi, \tau))$ (or equivalently with eigenvalues all equal to q^d or all equal to $-q^d$ on the d-th Tate twist of that space).

The Tate twist having no impact on the dimension, we end up trying to evaluate the dimension of the subspace of invariants:

$$\left(\left(\pi \rho_\ell \otimes \overline{\tau \rho_{\ell'}} \otimes \chi \tilde{\varphi} \right)_{\pi_1(\bar{V}, \bar{\mu})} \right)^{G^g(V/U)} \,.$$

As $\chi \tilde{\varphi}$ is trivial as a $\pi_1(\bar{V}, \bar{\eta})$-module, we have an isomorphism

$$\left(\pi \rho_\ell \otimes \overline{\tau \rho_{\ell'}} \otimes \chi \tilde{\varphi} \right)_{\pi_1(\bar{V}, \bar{\mu})} \simeq \left(\pi \rho_\ell \otimes \overline{\tau \rho_{\ell'}} \right)_{\pi_1(\bar{V}, \bar{\mu})} \otimes \chi \tilde{\varphi} \,.$$

Thanks to the assumption of linear disjointness, we have the isomorphism between the spaces of coinvariants

$$\left(\pi \rho_\ell \otimes \overline{\tau \rho_{\ell'}} \right)_{\pi_1(\bar{V}, \bar{\mu})} = \left([\pi, \bar{\tau}] \rho_{\ell, \ell'} \right)_{\pi_1(\bar{V}, \bar{\mu})} \simeq [\pi, \bar{\tau}]_{G_{\ell, \ell'}^{g, V}}$$

So, as we are now dealing with complex representations of finite groups, that last space of coinvariants coincides with the space of invariants $[\pi, \bar{\tau}]^{G_{\ell, \ell'}^{g, V}}$. As $\pi \in \Pi_\ell^*$ and $\tau \in \Pi_{\ell'}^*$, we can invoke [KoSieve, Lemma 3.4] to deduce that this space of invariants can only be non trivial in the case where $(\ell, \pi) = (\ell', \tau)$. As a consequence the dimension we are interested in is that of the subspace of the $G^g(V/U)$-invariants of

$$\left(\pi \rho_\ell \otimes \overline{\pi \rho_\ell} \right)_{\pi_1(\bar{V}, \bar{\mu})} \otimes \chi \tilde{\varphi} \,.$$

Applying once more the above arguments, we deduce that the dimension we actually need to compute is that of the space (recall that $\chi \tilde{\varphi}$ is a trivial $\pi_1(\bar{V}, \bar{\mu})$-module)

$$\left(\left(\pi \rho_\ell \otimes \overline{\pi \rho_\ell} \otimes \chi \tilde{\varphi} \right)^{\pi_1(\bar{V}, \bar{\mu})} \right)^{G^g(V/U)} \,.$$

To that purpose, we use the following lemma, which is purely representation theoretic.

Lemma 5. *Let G be a compact group, Ω a normal compact subgroup of G wtih abelian quotient K fitting the exact sequence*

$$1 \longrightarrow \Omega \longrightarrow G \longrightarrow K \longrightarrow 1 \,.$$

Let k be an algebraically closed field with characteristic zero, π a finite dimensional k-representation of G and χ a (degree 1) character of K. If $\bar{\pi}$ denotes the contragredient representation of π, then we have the isomorphism of G-modules

$$\left((\pi \otimes \bar{\pi} \otimes \chi)^\Omega \right)^K \simeq (\pi \otimes \bar{\pi} \otimes \chi)^G \,,$$

Proof. The space of invariants $(\pi \otimes \bar{\pi} \otimes \chi)^\Omega$ coincides with the projection of the restriction $(\pi \otimes \bar{\pi} \otimes \chi)_{|\Omega}$ on the trivial representation of Ω. Using Frobenius reciprocity, this space can also be written

$$\bigoplus_{\psi \in \hat{K}} (\pi \otimes \bar{\pi} \otimes \chi)(\psi) \,,$$

which is nothing but the sum of the ψ-components of $\pi \otimes \bar{\pi} \otimes \chi$ (seen as a G-module) over the characters ψ of K. This space can also be written

$$\bigoplus_{\psi \in \hat{K}} (\pi \otimes \bar{\pi})(\bar{\chi} \psi) \,.$$

9

Under this form, it is easy to deduce that the subspace of K-invariants of that representation is $(\pi \otimes \bar{\pi})(\bar{\chi})$, obtained by projecting on the trivial representation 1_K. Finally, this subspace can also be written $(\pi \otimes \bar{\pi} \otimes \chi)(1)$ which, by definition, is the space of invariants

$$(\pi \otimes \bar{\pi} \otimes \chi)^G \,.$$

$\square$

Thanks to the lemma, we can now give a useful expression for the dimension of the space of invariants we are interested in.

Lemma 6. *If $\left(\pi\rho_\ell \otimes \overline{\pi\rho_\ell} \otimes \chi\tilde{\varphi}\right)^{\pi_1(\bar{U},\bar{\eta})} \neq 0$, then there exists a character ψ_ℓ^χ of G_ℓ such that we have an isomorphism between the spaces of invariants*

$$\left([\pi,\bar{\pi}]\rho_\ell \otimes \chi\tilde{\varphi}\right)^{\pi_1(\bar{U},\bar{\eta})} \simeq \left([\pi,\bar{\pi}] \otimes \psi_\ell^\chi\right)^{G_\ell^g} \,.$$

Moreover the dimension of the latter space is

$$\gamma_\ell^{\pi,\chi} = |\{\psi \ \text{character of} \ G_\ell/G_\ell^g \mid \pi \simeq \pi \otimes \overline{\psi_\ell^\chi}\psi\}| \,.$$

Proof. Assuming the space of invariants we consider is not trivial, let us fix a nonzero $\pi_1(\bar{U},\bar{\eta})$-invariant vector v. We have

$$[\pi,\bar{\pi}](g)v = \overline{\chi\tilde{\varphi}}(g)v, \ \text{for all} \ g \in \pi_1(\bar{U},\bar{\eta}) \,.$$

For any g, we have $\chi\tilde{\varphi}(g) \in \{\pm 1\}$ and that quantity depends only on $\rho_\ell(g)$. Indeed, if g_1, g_2 are such that $\rho_\ell(g_1) = \rho_\ell(g_2)$, then the above relation yields $\chi\tilde{\varphi}(g_1) = \chi\tilde{\varphi}(g_2)$ since we chose $v \neq 0$. That observation enables us to define a character ψ_ℓ^χ of G_ℓ^g:

$$\psi_\ell^\chi(h) = \overline{\chi\tilde{\varphi}}(g), \ \text{where} \ h \in G_\ell^g \ \text{and} \ g \ \text{is such that} \ \rho_\ell(g) = h \,.$$

Notice that such a character ψ_ℓ^χ is trivial on $G_\ell^{g,V}$ simply because $\chi\tilde{\varphi}$ is trivial on $\pi_1(\bar{V},\bar{\mu})$. Thus, we can see it as a character of $G_\ell^g/G_\ell^{g,V}$ and it can be extended to a character of $G_\ell/G_\ell^{g,V}$ by making it act trivially on the possibly "missing" $\mathbf{Z}/2\mathbf{Z}$ factor (this is because we have the inclusions

$$\Omega(N,\mathbf{F}_\ell) \subset G_\ell^{g,V} \subset G_\ell^g \subset O(N,\mathbf{F}_\ell) \,,$$

and we know $O(N,\mathbf{F}_\ell)/\Omega(N,\mathbf{F}_\ell) \simeq \mathbf{Z}/2\mathbf{Z}/ \times \mathbf{Z}/2\mathbf{Z})$.

To prove the second part of the statement we need to determine the dimension of the space spanned by the vectors w satisfying

$$\pi \otimes \bar{\pi}(g)(w) = \overline{\psi_\ell^\chi(g)}w \,,$$

for all $g \in G_\ell^g$. Using Frobenius reciprocity once more, we can compute that dimension (equal to the multiplicity of the trivial character in the restriction of $\pi \otimes \bar{\pi} \otimes \psi_\ell^\chi$ to the group G_ℓ^g):

$$\langle \pi \otimes \bar{\pi} \otimes \psi_\ell^\chi; 1\rangle_{G_\ell^g} = \langle \pi \otimes \bar{\pi} \otimes \psi_\ell^\chi; \sum_\psi \psi\rangle_{G_\ell} \,,$$

where, in the last sum, ψ runs over the group of characters of the abelian group G_ℓ/G_ℓ^g.

As we have chosen $\pi \in \Pi_\ell^*$, the scalar product in the right hand side of the above equality is equal to the cardinality

$$\gamma_\ell^{\pi,\chi} = |\{\psi \ \text{character of} \ G_\ell/G_\ell^g \mid \pi \simeq \pi \otimes \overline{\psi_\ell^\chi}\psi\}| \,.$$

$\square$

Remark. We clearly have an injection

(8) $$\{\psi \ \text{character of} \ G_\ell/G_\ell^g \mid \pi \simeq \pi \otimes \overline{\psi_\ell^\chi}\psi\} \longrightarrow \hat{\Gamma}_\ell^\pi$$

$$\psi \mapsto \overline{\psi_\ell^\chi}\psi \,,$$

so that $\gamma_\ell^{\pi,\chi} \leqslant |\hat{\Gamma}_\ell^\pi|$ for any choice of $\pi \in \Pi_\ell^*$ and $\chi \in \widehat{G(V/U)}$.

To unify the notation, we set $\gamma_\ell^{\pi,\chi} = 0$ if $([\pi, \bar{\pi}]\rho_\ell \otimes \chi\tilde{\varphi})^{\pi_1(\bar{U},\bar{\eta})}$ is trivial. The following lemma enables us to determine completely the contribution of the trace of Frobenius on $H_c^{2d}(\bar{U}, \mathcal{F}_\chi(\pi,\pi))$.

Lemma 7. *Provided $H_c^{2d}(\bar{U}, \mathcal{F}_\chi(\pi,\pi))$ is non zero, there is a unique eigenvalue for the global geometric Frobenius acting on that space: it is either q^d or $-q^d$.*

Proof. It is enough to prove that the global geometric Frobenius acts on the space of coinvariants $(\pi\rho_\ell \otimes \bar{\pi}\rho_\ell \otimes \chi)_{\pi_1(\bar{U},\bar{\eta})}$ as either Id or $-$Id (so it acts on the d-th Tate twist by scalar multiplication by q^d or $-q^d$). From the arguments preceding Lemma 5 and Lemma 5 itself we know that the space of coinvariants we are interested in is isomorphic (as a Galois module) to the space of invariants

$$(\pi\rho_\ell \otimes \bar{\pi}\rho_\ell \otimes \chi\tilde{\phi})^{\pi_1(\bar{U},\bar{\eta})}.$$

That space of invariants can be seen as a $\hat{\mathbf{Z}}$-module for which we want to understand the action of its topological generator $d(\mathrm{Fr}_u) = -1$ for any $u \in U(F_q)$ such that $\tilde{\varphi}(\mathrm{Fr}_u) = \alpha$. Now from Lemma 6 that action is the same as that of $\mathrm{pr}_\ell(-1, \alpha)$ on $([\pi, \bar{\pi}] \otimes \psi_\ell^\chi)^{G_\ell^g}$.

We saw in the course of the proof of Lemma 6, that $([\pi, \bar{\pi}] \otimes \psi_\ell^\chi)^{G_\ell^g}$ decomposes as

$$\bigoplus \{\psi \text{ character of } G_\ell/G_\ell^g \mid \pi \simeq \pi \otimes \overline{\psi_\ell}\psi\}.$$

On each of these 1-dimensional summands $\mathrm{pr}_\ell(-1, \alpha)$ acts by multiplication by $\psi(\mathrm{pr}_\ell(-1), \alpha)$. For each $x \in Y_\ell$ and each ψ involved in the above sum, we have $\psi(x) = \psi(\mathrm{pr}_\ell(-1, \alpha))$. Now taking the trace on each side of the isomorphism defining the characters ψ we focus on, we get for all $x \in Y_\ell$:

$$\mathrm{Tr}\,\pi(x) = \mathrm{Tr}\,\pi(x)\overline{\psi_\ell^\chi}(x)\psi(x).$$

As we chose $\pi \in \Pi_\ell^*$, the function $\mathrm{Tr}\,\pi$ does not identically vanish on Y_ℓ and we get $\psi(\mathrm{pr}_\ell(-1, \alpha)) = \psi_\ell^\chi(\mathrm{pr}_\ell(-1, \alpha))$ for all ψ. The result follows from the fact that ψ_ℓ^χ takes its values in $\{\pm 1\}$. $\qquad\square$

Emphasizing the main term in the sum $W_\chi(\pi, \tau)$, we have just proven that

$$W_\chi(\pi, \tau) = \delta((\ell, \pi), (\ell', \tau))\gamma_\ell^{\pi,\chi} q^d + \sum_{i=0}^{2d-1} (-1)^i \mathrm{Tr}\big(\mathrm{Fr} \mid H_c^i(\bar{U}, \mathcal{F}_\chi(\pi, \tau))\big).$$

Now recall

$$W(\pi, \tau) = \big(|\hat{\Gamma}_\ell^\pi||\hat{\Gamma}_{\ell'}^\tau|\big)^{-1/2} |G(V/U)|^{-1} \sum_{\chi \in \widehat{G(V/U)}} \overline{\chi(\alpha)} W_\chi(\pi, \tau).$$

Setting

$$\varepsilon_\pi = \frac{1}{|G(V/U)|} \sum_\chi \big(\overline{\chi(\alpha)}(\gamma_\ell^{\pi,\chi}|\hat{\Gamma}_\ell^\pi|^{-1})\big),$$

and looking back at (8), we get the main term as stated in the proposition.

Applying Lemma 4 we finally get the full statement of the proposition. $\qquad\square$

Thanks to Proposition 3, we can deduce an upper bound for the large sieve constant Δ that in turn yields the following result:

Corollary 8. *With the same assumptions as in Proposition 3, let us denote $d' = N(N-1)/2$ the dimension of $\mathbf{O}(N)$ as an algebraic group, then we have*

$$|\{u \in U(\mathbf{F}_q) \mid \rho_\ell(\mathrm{Fr}_u) \notin \Theta_\ell \text{ for all } \ell \in \Lambda\}| \leqslant |G(V/U)|(q^d + Cq^{d-1/2}(L+1)^A)H^{-1},$$

where,

- *In case (1) of Proposition 3, $A = 7d'/2 + 1$ and C depends only on $\bar{U}$.*
- *In case (2) of Proposition 3, $A = 3d'/2 + 1$ and C depends only on the Euler-Poincaré characteristic of $\bar{U}$ and on the system $(\tilde{\mathcal{F}}_\ell)$ on $\bar{U}$.*

Proof. Let us fix $\alpha \in G(V/U)$. Combining (6) and Proposition 3, we get, in case (1) of Proposition 3,

$$|S(X_\alpha, \Theta; L)| \leqslant \max_{\ell, \pi} \Big\{ q^d + Cq^{d-1/2}(\dim \pi) \sum_{\ell', \tau} (\dim \tau) |G_{\ell, \ell'}| \Big\} H^{-1}\,,$$

whereas, in case (2) of Proposition 3,

$$|S(X_\alpha, \Theta; L)| \leqslant \max_{\ell, \pi} \Big\{ q^d + Cq^{d-1/2}(\dim \pi) \sum_{\ell', \tau} (\dim \tau) \Big\} H^{-1}\,.$$

Now we can use the following trivial inequalities

$$\dim \pi \leqslant \sqrt{|G_\ell|}\,, \quad \sum_{\tau \,\mathrm{irr}} \dim \tau \leqslant |G_{\ell'}|\,, \quad |G_{\ell, \ell'}| \leqslant |G_\ell||G_{\ell'}|\,,$$

where π is any irreducible representation of G_ℓ and τ runs over a set of representatives for the isomorphism classes of irreducible representations of $G_{\ell'}$. Doing so, we eventually get the upper bound:

$$|S(X_\alpha, \Theta; L)| \leqslant (q^d + Cq^{d-1/2}(L+1)^A)H^{-1}\,,$$

since we have

$$|G_\ell| \leqslant |O(N, \mathbf{F}_\ell)| \leqslant (\ell + 1)^{N(N-1)/2}\,.$$

To conclude the proof, we need only remark:

$$|\{u \in U(\mathbf{F}_q) \mid \rho_\ell(\mathrm{Fr}_u) \notin \Theta_\ell,\ \text{for all}\ \ell \leqslant L\}| = \sum_{\alpha \in G(V/U)} |S(X_\alpha, \Theta; L)|\,.$$

Thus the left hand side of the above equality can be bounded by

$$|G(V/U)| \max_{\alpha \in G(V/U)} |S(X_\alpha, \Theta; L)|\,.$$

Combining that with the upper bound for $|S(X_\alpha, \Theta; L)|$ we get the estimate we wanted. $\qquad\square$

Remark. It seems reasonable to hope that for any representation $\pi \in \Pi_\ell^*$ and any nontrivial χ, we have $\gamma_\ell^{\pi, \chi} = 0$. As we trivially see that $\gamma_\ell^{\pi, 1} = |\hat{\Gamma}_\ell^\pi|$, then this would enable us to set $\varepsilon_\pi = |G(V/U)|^{-1}$ for any π, which would be very useful both to save a power of 2 in the implied constant of Theorem 1 and for uniformity purposes. Indeed, without that kind of additional data, we cannot get rid of the constant $|G(V/U)|$ (i.e. of the dependency on the degree of the cover $V \longrightarrow U$) in corollary 8.

To deduce Theorem 1 from the above corollary, we need to give a lower bound for the constant H. As we are interested in uniformity issues (i.e. we would like the implied constant to be an absolute constant in our estimate, at least in the case where E is a Legendre curve), that lower bound needs to be explicit in terms of the common degree N of the L-functions studied.

3. STATEMENT AND PROOF OF THE MAIN RESULT

Applying the sieving machinery of the preceding section, we can prove a more general version of Theorem 1 in the context of Section 1. Indeed, beyond the question of the irreducibility of $L_{\mathrm{red},c}$ when averaging over c, we can investigate the question of the maximality of the Galois group of such a **Q**-polynomial.

3.1. **A stronger version of Theorem 1.** First, we need to understand why the setup of Section 1 fits the abstract geometric framework of Section 2.1. This is mostly due to Hall (see [Hall]). The parameter variety we are interested in is the affine curve U_g of Section 1, where g is a fixed element of F_{d-1}. We restrict ourselves to the curve U_g because we cannot guarantee that the condition $p \nmid |G_\ell^{g,V}|$ holds, as would be required by (1) of Proposition 3 if we wanted to work with the variety F_d.

With notation as in Section 1, there is, for each ℓ a unique lisse $\mathbf{F}_\ell$-sheaf denoted $\mathcal{T}_{d,\ell}$ whose fiber over any $f \in F_d(\mathbf{F}_q)$ is $\mathcal{V}_{f,\ell}$. That sheaf can be restricted to the curve U_g and this gives rise, for a geometric point $f(t) = (c-t)g(t) \in F_d(\overline{\mathbf{F}_q})$ to a representation:

$$\pi_1(U_g, \bar{c}) \longrightarrow GL(\mathcal{V}_{f,\ell}),$$

where $\bar{c}$ is a geometric point over c.

From what we saw at the end of Section 1.1, we know that the image of that representation sits in the orthogonal group $O(\mathcal{V}_{f,\ell})$ (with respect to the symmetric pairing given by Poincaré duality). That means both the arithmetic and the geometric monodromy groups of $\mathcal{T}_{d,\ell}$ are subgroups of $O(\mathcal{V}_{f,\ell})$. As explained by Hall in [Hall, Section 2], the system of sheaves $(\mathcal{T}_{d,\ell})_\ell$ restricted to U_g forms a compatible system in the sense of Definition 2. Indeed we have

$$L_{\mathrm{red}}(E_f/K; T) \equiv \det(1 - T\mathrm{Fr}_q \mid \mathcal{V}_{f,\ell}) \,(\mathrm{mod}\,\ell),$$

which of course is a crucial identity for us as we want to study $L_{\mathrm{red}}(E_f/K; T)$ via sieve methods.

Finally we need to understand why there exists an étale Galois cover $V_g \longrightarrow U_g$ satisfying the properties stated in Section 2.1. That is in fact a reformulation of Hall's Theorem 6.6 in [Hall]. The following lemma, which was explained to the author by C. Hall, provides us with a precise version of the property we need.

Lemma 9. *With notation as above, if we assume that $d = \deg g + 1 \geqslant d_0(E)$ and $\ell \geqslant \ell_0(E)$, then there exists an étale Galois cover $V_g \longrightarrow U_g$, with Galois group $G(V_g/U_g)$ an elementary 2-group, such that, if we denote by ρ_ℓ the representation which "is" $\mathcal{T}_{d,\ell}$, we have*

$$\rho_\ell(\pi_1(\overline{V_g}, \bar{\mu})) = \Omega(N, \mathbf{F}_\ell),$$

and

$$\rho_{\ell,\ell'}(\pi_1(\overline{V_g}, \bar{\mu})) = \Omega(N, \mathbf{F}_\ell) \times \Omega(N, \mathbf{F}_{\ell'}),$$

for $\ell \neq \ell'$.

Moreover we can choose

$$\ell_0(E) = \max\big(13, \max\{p' \ prime \mid v_{p'}(-\mathrm{ord}_P(j(E))) > 0 \ for \ some \ P \in \mathbf{F}_q[t] \ irreducible\}\big).$$

Proof. Let $U_{\ell,g} \longrightarrow U_g$ be the cover with Galois group G_ℓ. Because $\mathcal{T}_{d,\ell}$ (or ρ_ℓ) has big geometric monodromy for d and ℓ large enough (see [Hall, Th. 6.3]), the group G_ℓ^g (which is a subgroup of G_ℓ) contains the derived group $\Omega(N, \mathbf{F}_\ell)$ of the orthogonal group as soon as ℓ is sufficiently large. If $W_{\ell,g} \longrightarrow U_g$ is the subcover corresponding to $\Omega(N, \mathbf{F}_\ell)$ then $W_{\ell,g} \longrightarrow U_g$ is Galois with group a subgroup of $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Thus if we define V_g to be the compositum of these covers, the cover $V_g \longrightarrow U_g$ we get is still Galois with group an elementary 2-group. Now $\Omega(N, \mathbf{F}_\ell)$ has no non trivial abelian quotient (see e.g. [D, Prop. 10]), so applying Goursat-Ribet's Theorem (see e.g. [Chav, Prop. 5.1]), we deduce that the covers $U_{\ell,g} \longrightarrow W_{\ell,g}$ and $V_g \longrightarrow W_{\ell,g}$ are disjoint; in particular, if $V_{\ell,g}$ is the compositum of $V_g \longrightarrow W_{\ell,g}$ and $U_{\ell,g} \longrightarrow W_{\ell,g}$, then the Galois group of $V_{\ell,g} \longrightarrow W_{\ell,g}$ is that of $U_{\ell,g} \longrightarrow W_{\ell,g}$ which is precisely $\Omega(N, \mathbf{F}_\ell)$. In particular, as $\Omega(N, \mathbf{F}_\ell)$ has no non trivial abelian quotient, we deduce $\rho_\ell(\pi_1(\overline{V_g}, \bar{\mu})) = \Omega(N, \mathbf{F}_\ell)$.

The statement of linear disjointness follows by invoking once more Goursat-Ribet's Theorem.

As far as the minimal value for ℓ is concerned, we exploit the remark following [Hall, Lemma 6.1]. Besides the fact that $\ell \geqslant 5$, there are two conditions needed for Hall's Theorem to apply: ℓ should not divide the multiplicity of any irreducible polynomial in $\mathbf{F}_q[t]$ appearing as a factor of the denominator of the j-invariant of E, and if $f(t) = (c-t)g(t)$ then the Galois group of the torsion field $K(E_f[\ell])$ over K contains $SL(2, \mathbf{F}_\ell)$.

This last condition can be made explicit thanks to a result due to A. Cojocaru and C. Hall (see [CH, Th. 1]) about the uniformity (in the function field case) of Serre's result on the surjectivity of mod ℓ Galois representations of elliptic curves. Their Theorem gives a very explicit lower bound for the first prime ℓ for which surjectivity holds, and this bound depends only on the genus of the function field over which the elliptic curve considered is defined. Applying their

formula in our case (i.e. in the case of a rational function field), we obtain that the surjectivity property holds as soon as $\ell \geqslant 13$.

$\square$

Now Corollary 8 may be applied in the framework of Section 1.1, that means with $U = U_g$ and ρ_ℓ corresponding for each ℓ to the restriction of $\mathcal{T}_{d,\ell}$ to U_g. For a suitable choice of sieving sets Θ_ℓ we might then obtain a proof of Theorem 1, provided we can produce a good enough uniform lower bound for H. However we can do better than just investigating the irreducibility of L-functions when averaging over $U_g(\mathbf{F}_q)$. Indeed as noticed by Kowalski in [KoSieve, 8.6] and as we did in [J] in the context of random walks on integral points of orthogonal groups, we can get quantitative information on the maximality of the Galois group of the $\mathbf{Q}$-polynomial $L_{\mathrm{red}}(E_c/K; T)$, when c runs over the set of $\mathbf{F}_q$-rational points of U_g.

First, the functional equation (1) imposes the Galois group of $L_{\mathrm{red}}(E_c/K; T)$ to be strictly smaller than the full symmetric group $\mathfrak{S}_{N_{\mathrm{red}}}$. Indeed that Galois group acts on pairs of roots $\{\alpha_i, \alpha_{N_{\mathrm{red}}/2}\}$ for $1 \leqslant i \leqslant N_{\mathrm{red}}/2 + i$. We deduce that the maximal Galois group that the $\mathbf{Q}$-polynomial $L_{\mathrm{red}}(E_c/K; T)$ can have is the group denoted $W_{N_{\mathrm{red}}}$. This group coincides with the Weyl group of the algebraic group $\mathbf{O}(N)$. That is an instance of a much more general principle according to which the Galois group of the characteristic polynomial of an integral point of any reductive group $\mathbf{G}/\mathbf{Q}$ should "generically" coincide with the Weyl group of $\mathbf{G}$ (at least if $\mathbf{G}/\mathbf{Q}$ is split). Such a question is investigated in [JKZ] in the case of a split model over $\mathbf{Q}$ of the exceptional group $\mathbf{E}_8$, in [KoSieve, Chap. 7] for $\mathbf{SL}(n)$ and $\mathbf{Sp}(2g)$ and in [J] for the orthogonal group with respect to an indefinite quadratic form.

As a consequence, it seems fair to say that the $\mathbf{Q}$-polynomial $L_{\mathrm{red}}(E_c/K; T)$ has *small Galois group* if the Galois group of its splitting field over $\mathbf{Q}$ is strictly contained in $W_{N_{\mathrm{red}}}$. Now the generalized version of Theorem 1 we shall prove is the following:

Theorem 10. *With notation as in Section 1, let $L_{\mathrm{red},c}$ denote the reduced L-function of the quadratic twist E_c of E. For $N \geqslant 5$, $d = \deg(g) + 1 \geqslant d_0(E)$, and $q \geqslant q_0(E)$, we have*

$$|\{c \in \mathbf{A}^1(\mathbf{F}_q) \mid g(c)m(c) \neq 0 \text{ and } L_{\mathrm{red},c} \text{ has small Galois group }\}| \ll N^2 |G(V_g/U_g)| q^{1-\gamma} \log q,$$

where the implied constant depends only on $j(E)$ (e.g. it does not depend on N, and q could be replaced by q^n for any $n \geqslant 1$), and where we can choose $2\gamma^{-1} = 7N^2 - 7N + 4$.

Besides the large sieve inequality contained in the statement of Corollary 8, the other ingredient we need in order to prove Theorem 10 consists in a suitable choice of families Θ and, for each such family, a good enough uniform lower bound for the constant H. As the Galois groups we are investigating are subgroups of the Weyl group $W_{N_{\mathrm{red}}}$, the choice for the families Θ is almost the same as in our previous work [J, Lemma 20]. The only thing that changes here is the number of left cosets of $O(N, \mathbf{F}_\ell)$, with respect to $\Omega(N, \mathbf{F}_\ell)$, that we consider. Indeed, in loc. cit., we were only working with matrices whose determinant was 1, namely elements of $SO(n,m)(\mathbf{Z})$. In that case the spinor norm is the only invariant that discriminates a left coset from another. Here we also have to handle the cosets given by $(\det = -1, \mathrm{N}_{\mathrm{Spin}} = \pm 1)$. To describe the families Θ we choose, we need first to recall a few notations from [J]: we consider the set of polynomials

$$M_{N,\ell} = \left\{ 1 + b_1 T + \cdots + b_N T^N \mid b_i \in \mathbf{F}_\ell, b_N^2 = 1 \text{ and } b_{N-i} = b_N b_i, \text{ if } 0 \leqslant i \leqslant \lfloor N/2 \rfloor \right\}.$$

For a fixed left coset $\alpha_\ell G_\ell^{g,V} \subset O(N, \mathbf{F}_\ell)$, the integer N_{red} is well defined as the degree of the reduced characteristic polynomial of any matrix in that coset in the sense of (2), namely

$$N_{\mathrm{red}} = \begin{cases} N \text{ if } N \text{ is even and } \det \alpha_\ell = 1, \\ N - 2 \text{ if } N \text{ is even and } \det \alpha_\ell = -1, \\ N - 1 \text{ if } N \text{ is odd}. \end{cases}$$

14

Thus we can define a family of sieving sets $(\Theta_\ell)_\ell$ such that $\Theta_\ell \subset Y_\ell = \alpha_\ell G_\ell^{g,V}$, via the formula

$$\Theta_\ell = \{g \in O(N, \mathbf{F}_\ell) \mid (\det, \mathrm{N}_{\mathrm{Spin}})(g) = (\varepsilon_\ell^{(1)}, \varepsilon_\ell^{(2)}), \det(1 - Tg)_{\mathrm{red}} \in \tilde{\Theta}_\ell\}\,,$$

where $\tilde{\Theta}_\ell$ is for each ℓ a fixed subset of $M_{N_{\mathrm{red}}, \ell}$.

Now our choice for families of sieving sets corresponds to the following sets of polynomials and values for $\varepsilon_\ell^{(1)}, \varepsilon_\ell^{(2)}$.

(1) The set $\Theta_\ell^{(1)}$ corresponds to the set of polynomials $\tilde{\Theta}_\ell^{(1)}$
- which are either irreducible *if N is odd or if N is even and $\varepsilon_\ell^{(1)} = -1$*, or irreducible with a fixed value modulo nonzero squares of $\mathbf{F}_\ell$ at -1 and satisfy $\mathrm{disc}(f) = \mathrm{disc}(Q)$ *if N is even, $\varepsilon_\ell^{(1)} = 1$, and $O(N_{\mathrm{red}}, \mathbf{F}_\ell) = O(N, \mathbf{F}_\ell)$ is nonsplit,*
- which factor as a product of two distinct monic irreducible polynomials of degree $N_{\mathrm{red}}/2$ *if $\varepsilon_\ell^{(1)} = 1$, $O(N_{\mathrm{red}}, \mathbf{F}_\ell)$ is split and $\ell \equiv 1 \,(\mathrm{mod}\,4)$,*
- which factor as a product of an irreducible monic quadratic polynomial and an irreducible polynomial of degree $N_{\mathrm{red}} - 2$ *if $\varepsilon_\ell^{(1)} = 1$, $O(N_{\mathrm{red}}, \mathbf{F}_\ell)$ is split and $\ell \equiv 3 \,(\mathrm{mod}\,4)$.*

(2) Let $\tilde{\Theta}_\ell^{(2)}$ be the set of polynomials f in $M_{N_{\mathrm{red}}, \ell}$ with a fixed value modulo nonzero squares of $\mathbf{F}_\ell$ at -1, which satisfy $\mathrm{disc}(f) = \mathrm{disc}(Q)$ and which factor as a product of a monic quadratic polynomial with distinct monic irreducible polynomials of odd degree.

(3) Let $\tilde{\Theta}_\ell^{(3)}$ be the set of polynomials f in $M_{N_{\mathrm{red}}, \ell}$ with a fixed value modulo nonzero squares of $\mathbf{F}_\ell$ at -1, which satisfy $\mathrm{disc}(f) = \mathrm{disc}(Q)$ and with associated polynomial h (such that $f = x^n h(x + x^{-1})$) being separable with at least one factor of prime degree $> N_{\mathrm{red}}/4$.

(4) Let $\tilde{\Theta}_\ell^{(4)}$ be the set of polynomials f in $M_{N_{\mathrm{red}}, \ell}$ with a fixed value modulo nonzero squares of $\mathbf{F}_\ell$ at -1, which satisfy $\mathrm{disc}(f) = \mathrm{disc}(Q)$ and with associated polynomial h being separable with one irreducible quadratic factor and no other irreducible factor of even degree.

The above choices are justified by [KoZeta, Lemma 7.1(iii)] and the discussion following (8.4) in loc. cit. It is indeed proven therein that if the four conjugacy classes of $W_{N_{\mathrm{red}}}$, that are implicitly emphasized by the four choices above, are contained in a subgroup of $W_{N_{\mathrm{red}}}$ then that subgroup is the full group $W_{N_{\mathrm{red}}}$. Notice here that finding a good family $\Theta^{(1)}$ is quite an issue, though its purpose is "as simple as" detecting the irreducibility of the $\mathbf{Q}$-polynomial we investigate (namely the reduced L-function of a quadratic twist of the elliptic curve E). We refer the reader to [J, Sections 2 and 3] for details and explanations regarding this particular feature and to [Ka, end of Section 7] for the trick of looking both at reductions of the type ($\mathbf{F}_\ell$-irreducible of degree 2)($\mathbf{F}_\ell$-irreducible of degree $N_{\mathrm{red}} - 2$) and ($\mathbf{F}_\ell$-irreducible of degree $N_{\mathrm{red}}/2$)(a different $\mathbf{F}_\ell$-irreducible of degree $N_{\mathrm{red}}/2$) to detect $\mathbf{Q}$-irreducibility.

As explained earlier, we need uniform lower bounds (in terms of the degree N) for each constant H corresponding to our different choices of families Θ. Those bounds are essentially provided by the following Lemma:

Lemma 11. *Suppose $N \geqslant 5$. For the first three families of sieving sets above, the following estimates hold for $\ell \geqslant \ell_0(N)$:*

$$\frac{|\Theta_\ell^{(1)}|}{|\Omega(N, \mathbf{F}_\ell)|} \geqslant \frac{1}{4N^2}\,, \qquad \frac{|\Theta_\ell^{(2)}|}{|\Omega(N, \mathbf{F}_\ell)|} \geqslant \frac{1}{5N}\,, \qquad \frac{|\Theta_\ell^{(3)}|}{|\Omega(N, \mathbf{F}_\ell)|} \geqslant \frac{7}{3N}\,.$$

For the family fo sieving sets $(\Theta_\ell^{(4)})$, we have, for $\ell \geqslant \ell_0(N)$,

$$\frac{|\Theta_\ell^{(4)}|}{|\Omega(N, \mathbf{F}_\ell)|} \geqslant \frac{1}{9N(N-6)} \ \text{if } N_{\mathrm{red}} \geqslant 10, \ \text{and} \ \frac{|\Theta_\ell^{(4)}|}{|\Omega(N, \mathbf{F}_\ell)|} \geqslant \frac{1}{N^2}, \text{otherwise}\,.$$

Proof. For $\Theta_\ell^{(1)}$ the major part of the argument is contained in the proof of [J, Lemma 20]. From the estimates proved in loc. cit., we easily deduce, in the case where $N = N_{\mathrm{red}}$ is even, $\varepsilon_\ell^{(1)} = 1$

15

and the orthogonal group $O(N, \mathbf{F}_\ell)$ is nonsplit, the following asymptotic expansion:

$$\frac{|\Theta_\ell^{(1)}|}{|\Omega(N, \mathbf{F}_\ell)|} \geqslant \frac{1}{2N} - \frac{N(N-1) + 4N + 4}{4N\ell} + O\Big(\frac{N^3}{\ell^2}\Big),$$

with an absolute implied constant. Thus

$$\frac{|\Theta_\ell^{(1)}|}{|\Omega(N, \mathbf{F}_\ell)|} \geqslant \frac{1}{3N},$$

for $\ell \geqslant \ell_0(N)$. Moreover, the results of Katz ([Ka, Section 6]) provide us with the following lower bounds:

$$\frac{|\Theta_\ell^{(1)}|}{|\Omega(N, \mathbf{F}_\ell)|} \geqslant \frac{1}{4(N-2)},$$

as soon as $\ell \geqslant \max(7, N/2 - 1)$, if N is even and $\varepsilon_\ell^{(1)} = -1$ (this is [Ka, Lemma 6.3]). Other lemmas from loc. cit. are also used in [J, Lemma 20] to prove

$$\frac{|\Theta_\ell^{(1)}|}{|\Omega(N, \mathbf{F}_\ell)|} \geqslant \frac{1}{4N^2},$$

in the split case and assuming $\varepsilon_\ell^{(1)} = 1$, and

$$\frac{|\Theta_\ell^{(1)}|}{|\Omega(N, \mathbf{F}_\ell)|} \geqslant \frac{1}{2N-2},$$

as soon as $\ell \geqslant \max(7, (N-1)/2)$ if N is odd.

Overall, we obtain the lower bound stated as soon as $N \geqslant 3$.

As far as $\Theta_\ell^{(2)}$ is concerned, we deduce from the formula of [J, Proof of Lemma 20] that

$$\frac{|\Theta_\ell^{(2)}|}{|\Omega(N, \mathbf{F}_\ell)|} \geqslant \frac{1}{4N} - \frac{3N^2 + 3N + 1}{24N\ell} + O\Big(\frac{N^3}{\ell^2}\Big),$$

with an absolute implied constant. So for $\ell \geqslant \ell_0(N)$,

$$\frac{|\Theta_\ell^{(2)}|}{|\Omega(N, \mathbf{F}_\ell)|} \geqslant \frac{1}{5N}.$$

Finally for $\Theta^{(3)}$ and $\Theta^{(4)}$, loc. cit. provides us on the one hand with:

$$\frac{|\Theta_\ell^{(3)}|}{|\Omega(N, \mathbf{F}_\ell)|} \geqslant \frac{7}{2N} - \frac{7N^2 + 23N + 28}{4N\ell} + O\Big(\frac{N^3}{\ell^2}\Big),$$

as soon as $N \geqslant 5$ and with an absolute implied constant, and on the other hand, for $N_{\text{red}} \geqslant 10$, with

$$\frac{|\Theta_\ell^{(4)}|}{|\Omega(N, \mathbf{F}_\ell)|} \geqslant \frac{1}{8(N-6)} - \frac{5N(N-1) + 1}{80(N-6)\ell} + O\Big(\frac{N^3}{\ell^2}\Big),$$

with an absolute implied constant. The last inequality is obtained by combining the expression for $|\tilde{\Theta}_\ell^{(4)}|$ in [J, Proof of Lemma 20] and Lemma 16 of loc. cit. From the above expressions we deduce:

$$\frac{|\Theta_\ell^{(3)}|}{|\Omega(N, \mathbf{F}_\ell)|} \geqslant \frac{7}{3N}, \qquad \frac{|\Theta_\ell^{(4)}|}{|\Omega(N, \mathbf{F}_\ell)|} \geqslant \frac{1}{9(N-6)},$$

for $\ell \geqslant \ell_0(N)$, with the second inequality holding if we assume $N_{\text{red}} \geqslant 10$. To conclude, we need to handle separately the case where $N_{\text{red}} \leqslant 8$ (i.e. $N_{\text{red}} \in \{4, 6, 8\}$). To that end we use once more the corresponding formulæ contained in the proof of [J, Lemma 20] as well as [J, Lemma 16]. It is then straightforward to derive, for $\ell \geqslant \ell_0(N)$,

$$|\Theta_\ell^{(4)}||\Omega(N, \mathbf{F}_\ell)|^{-1} \geqslant \frac{1}{N^2},$$

from these references. $\qquad\square$

Remarks. (i) From the lower bound for $|\Theta_\ell^{(1)}||\Omega(N,\mathbf{F}_\ell)|^{-1}$ in Lemma 11, we deduce a new proof of (2) of [KoTwist, Lemma 5.1]. In loc. cit. the author suggests that such a result should follow from an adaptation to the orthogonal case of the method used by Chavdarov in [Chav, Th. 3.5 attributed to Borel] to prove that the matrices in $Sp(2g,\mathbf{F}_\ell)$ are equidistributed in the subsets containing matrices having a common characteristic polynomial. As explained in [J, Section 2], such an adaptation is not straightforward at all (e.g. the analog equidistribution statement does not hold in full generality) because of the many complications due to the lack of good topological properties of the orthogonal group as an algebraic group.

(ii) To get a deeper understanding of the issue discussed in (i), we easily see that the crucial question is: given a quadratic (resp. symplectic) $2n$-dimensional space (V,Q) over $\mathbf{F}_\ell$ and a polynomial f satisfying (1) (resp. a self reciprocal f), is it true that there is an $M \in O(2n,\mathbf{F}_\ell)$ (resp. $M \in Sp(2n,\mathbf{F}_\ell)$) such that $\det(1-TM) = f$?

For simplicity we assume that we always choose a separable f and, in the orthogonal case, that f is monic. In that case we are looking for a matrix in $SO(2n,\mathbf{F}_\ell)$. The strategy used by Chavdarov is to consider this question as a rationality problem: does the set of $\overline{\mathbf{F}_\ell}$-points in $\mathbf{SO}(2n)$ (resp. $\mathbf{Sp}(2n)$) with common characteristic polynomial f contain an $\mathbf{F}_\ell$-point? Chavdarov considers the centralizer $C_{\bar{M}}$ under $Sp(2n,\overline{\mathbf{F}_\ell})$ of an element $\bar{M} \in Sp(2n,\overline{\mathbf{F}_\ell})$ with characteristic polynomial f. Because $\mathbf{Sp}(2n)$ is simply connected $C_{\bar{M}}$ is connected and thus is equipped with Lang's isogeny. This observation yields an $\mathbf{F}_\ell$-point with characteristic polynomial f in the symplectic case. As $\mathbf{SO}(2n)$ is not simply connected that method cannot be directly applied in the orthogonal case. Indeed a result of Steinberg (see [SpSt, II Cor. 4.4]) asserts that non connected centralizers will occur as soon as the group acting is not simply connected. Moreover we cannot "lift" that method to the simply connected cover $\mathbf{Spin}(2n)$ of $\mathbf{SO}(2n)$ because the possibilty to produce an element in $\mathrm{Spin}(2n,\mathbf{F}_\ell)$ from an isometry in $SO(2n,\mathbf{F}_\ell)$ depends on the spinor norm of the isometry (see [Ka, Rem. 6.1]).

The spinor norm turns out to be the right invariant that enables us to answer the question in the orthogonal case. First a result of Zassenhaus (see [Za, (2.1) and p. 446]) asserts that the spinor of an isometry with characteristic polynomial f has spinor norm $f(-1)$ modulo squares (provided -1 is not a root of f). Second, an easy computation yields $\mathrm{disc}(f) = (-1)^n f(1) f(-1)$ (see [E, Th. 1 and Th. 2]). Finally, a result of Baeza (see [Ba, prop. 3.6 and Th. 3.7] and also [GM, prop. A.3]) asserts that an $M \in SO(2n,\mathbf{F}_\ell)$ with prescribed characteristic polynomial f exists if and only if $\mathrm{disc}(Q) = \mathrm{disc}(f)$ (modulo squares).

The above condition on equality of discriminants can be restated in the framework of Rodriguez-Villegas' unpublished note [R]: indeed in loc. cit., the author gives a very general and intrinseque construction that relates to the present question. If we restrict to the case of finite fields, that construction implies the following: let $\varepsilon = \pm 1$ and consider two coprime polynomials $f,g \in \mathbf{F}_\ell[T]$ with degree $2n$ such that f is self reciprocal and $T^{2n}g(T^{-1}) = -\varepsilon g(T)$. Then one can produce a $2n$-dimensional quadratic (resp. symplectic) space if $\varepsilon = 1$ (resp. $\varepsilon = -1$) and two elements A, B in $O(2n,\mathbf{F}_\ell)$ (resp. $Sp(2n,\mathbf{F}_\ell)$) with respective characteristic polynomials f and g. Rodriguez-Villegas shows that if $\varepsilon = -1$ and given a polynomial f as above, we can always produce a suitable polynomial g, reproving in turn Chavdarov's result [Chav, Lemma 3.4]. Now if $\varepsilon = 1$ the quadratic space we end up with has discriminant equal to the resultant $\mathrm{Res}(f,g)$ of f and g. Combining that with the facts mentioned above we deduce that given f, finding a suitable g is equivalent to solving the equation $\mathrm{Res}(f,g) = \mathrm{disc}(f)$ for g.

(iii) The smallest prime $\ell_0(N)$ for which the estimates of Lemma 11 hold can be made explicit. Indeed, exploiting the asymptotic expansions we used in the proof, we deduce by inspection that all the inequalities hold as soon as $\ell \geqslant 5N^2$.

(iv) It is very likely (though the author could not come up with a satisfactory statement covering all the different cases) that a clever adaptation and/or combination of Katz's computations [Ka, Lemmas 6.2 through 6.6] would yield similar estimates as those given in Lemma 11.

Note that, in performing such a computation, it might be more convenient to use the criterion [KoZeta, Lemma 7.1*(ii)*] rather than [KoZeta, Lemma 7.1*(iii)*] for a subgroup of $W_{N_{\mathrm{red}}}$ to be equal to the full group.

To each of the families $\Theta^{(i)}$ of Lemma 11, where $1 \leqslant i \leqslant 4$, corresponds a conjugacy class, say $\Theta^{\sharp(i)}$, of $W_{N_{\mathrm{red}}}$. So with notation as in Theorem 10, we have

$$|\{c \mid L_{\mathrm{red},c} \text{ has small Galois group }\}| \leqslant \sum_{1 \leqslant i \leqslant 4} |\{c \mid \mathrm{Gal}(L_{\mathrm{red},c}/\mathbf{Q}) \cap \Theta^{\sharp(i)} = \emptyset\}| \,,$$

where the parameter c runs over the elements of $\mathbf{A}^1(\mathbf{F}_q)$ such that $f(t) = (c - t)g(t) \in F_d(\mathbf{F}_q)$. The explanations following [KoZeta, (8.4)] and justifying our choice of families $\Theta^{(i)}$ enable us to deduce:

$$|\{c \mid L_{\mathrm{red},c} \text{ has small Galois group }\}| \leqslant \sum_{1 \leqslant i \leqslant 4} |\{u \in U_g(\mathbf{F}_q) \mid \rho_\ell(\mathrm{Fr}_u) \notin \Theta_\ell^{(i)} \text{ for } \ell_0(E) \leqslant \ell \leqslant L\}| \,,$$

where $\ell_0(E)$ is chosen in such a way that both Lemma 9 and Lemma 11 hold and $L \geqslant \ell_0(E)$ is a fixed parameter (in particular, because of point *(ii)* of the above remark, we can use the inequalities of Lemma 11 provided $L \geqslant 5N^2$).

Set

$$\Lambda = \{\ell \text{ prime} \mid \ell_0(E) \leqslant \ell \leqslant L\} \,.$$

Applying Corollary 8, Lemma 11 and the Prime Number Theorem, we get

$$|\{c \mid L_{\mathrm{red},c} \text{ has small Galois group }\}| \ll N^2 |G(V_g/U_g)| L^{-1} \log L (q + Cq^{1/2}(L+1)^A) \,,$$

with an implied constant depending only on $j(E)$.

Remark. Note that, when applying the Prime Number Theorem, a natural constraint is imposed on L: since we only consider primes greater than $5N^2$, we need to choose (roughly) $L \gg N^2 \log(N)$ (see [KoZeta, end of Section 8]). As explained in loc. cit. this condition can in fact be removed by modifying appropriately the implied constant in the above inequality. Indeed, that inequality becomes trivial as soon as $N^2 \geqslant L(\log L)^{-1}$.

Setting $L = q^{1/2A}$ we deduce

$$|\{c \mid L_{\mathrm{red},c} \text{ has small Galois group }\}| \ll N^2 |G(V_g/U_g)| q^{1-1/2A} \log q \,,$$

with an implied constant depending only on $j(E)$.

Looking back at the definition of A (see Corollary 8), we see that

$$2A = \frac{7}{2}N^2 - \frac{7}{2}N + 2 \,,$$

so that the proof of Theorem 10 is complete.

Remark. Note that we need to assume that the common degree d of the twisting polynomials is large enough in order to apply Corollary 8. The degree N of the L-functions we study is related to d (sometimes in a very explicit way, see the following section), as (3) shows quite obviously. As a consequence, we need to have $L = q^{1/2A}$ big enough (i.e. greater than the parameter $\ell_0(E)$ of Lemma 9) and simultaneously d (and thus N) big enough. This is of course always possible if q is big enough and this is why we assume $q \geqslant q_0(E)$ in the statement of Theorem 1 and Theorem 10. This might be a bit unsatisfactory as the smallest suitable value of q is not clear, however we can also usefully notice that the estimate of Theorem 10 is trivial for small values of q (say if $N^2 |G(V_g/U_g)| \gg q^{1/2A} \log(q)^{-1}$). In the next subsection though, we see that in the case where E is a Legendre curve, a much more precise answer to that question arises from the resolution of the uniformity issue.

3.2. Uniformity in the case of a Legendre curve. In this last subsection we focus on the case where E/K is a Legendre curve. Keeping the notation $K = \mathbf{F}_q(t)$ we let E be the elliptic curve over K defined as the projective compactification of the affine curve given by

$$y^2 = x(x-1)(x-t).$$

The affine variety F_d can be seen in that case as the set of polynomials with degree d in $\overline{\mathbf{F}_q}[t]$ that are coprime to $t(t-1)$. Lemma 6.7 of [Hall] provides us on the one hand with the dimension N of the space $\mathcal{V}_{f,\ell}$:

$$(9) \qquad\qquad N = \left\{ \begin{array}{l} 2d \text{ if } d \text{ is even}, \\[2mm] 2d - 1 \text{ if } d \text{ is odd}, \end{array} \right.$$

and on the other hand with the fact that Lemma 9 holds for any $d \geqslant 2$ and any $\ell \geqslant 5$. So if we fix a polynomial $g \in F_{d-1}$ and a Galois cover $V_g \longrightarrow U_g$ satisfying the hypotheses of Lemma 9, we can state the following result which can be seen as a uniform quantitative version of Katz's Theorem in the special case (stated in the introduction) of twists of Legendre curves:

Theorem 12. *Let E/K be the Legendre curve defined as above. With the same notation as in Theorem 10 we have, for any $d \geqslant 3$ and any power q of p,*

$$|\{c \in \mathbf{A}^1(\mathbf{F}_q) \mid g(c) \neq 0, c \neq 0, 1 \text{ and } L_{\mathrm{red},c} \text{ has small Galois group }\}| \ll d^2 |G(V_g/U_g)| q^{1-\gamma} \log q,$$

with an absolute implied constant and where we can choose $2\gamma^{-1} = 7N^2 - 7N + 4$ (the link between N and d being given by (9)).

Proof. The statement follows directly from the combination of Theorem 10, Lemma 6.7 in [Hall] and the fact that the denominator of the j-invaraint of the Legendre curve E does not have any irreducible factor appearing with multiplicity greater than 2. $\qquad\square$

References

[Ba]   R. Baeza : *Discriminants of polynomials and of quadratic forms*, J. Algebra 72, (1981), 17–28.

[Chav] N. Chavdarov: *The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy*, Duke Math. J. 87 (1997), 151–180.

[CH]   A. Cojocaru and C. Hall: *Uniform results for Serre's theorem for elliptic curves*, Int. Math. Res. Not. (2005), no. 50, 3065–3080.

[DeW]   P. Deligne: *La conjecture de Weil II*, Inst. Hautes Études Sci. Publ. Math. No. 52 (1980), 137–252.

[De]   P. Deligne: *Cohomologie étale*, S.G.A $4\frac{1}{2}$, L.N.M. 569, Springer Verlag 1977.

[D]   J. Dieudonné : *Sur les groupes classiques*, Hermann, (1958).

[E]   B. H. Edwards : *Rotations and discriminants of quadratic spaces*, Lin. and Multilin. Algebra 8, (1980), 241–246.

[G]   A. Grothendieck: *Formule de Lefschetz et rationalité des fonctions L*, Séminaire Bourbaki, (1964–65), North Holland (1968), exp. 279, 1–15.

[GM]   B. Gross and C. Mc Mullen: *Automorphisms of even unimodular lattices and unramified Salem numbers*

[Hall] C. Hall: *Big orthogonal or symplectic monodromy mod ℓ*, Duke Math. J. 141 (2008) 179–203.

[J]   F. Jouve: *The large sieve and random walks on left cosets of arithmetic groups*, submitted. `arXiv:math.NT/0811.1793`

[JKZ]   F. Jouve, E. Kowalski and D. Zywina: *An explicit integral polynomial whose splitting field has Galois group $W(E8)$*, to appear, J. Théor. Nombres Bordeaux.`arXiv:math.NT/0801.1733`

[Ka]   N. M. Katz : *Report on the irreducibility of L-functions*, to appear, (volume in honour of S. Lang).

[KoZeta] E. Kowalski : *The large sieve, monodromy and zeta functions of curves*, J. reine angew. Math 601 (2006), 29–69.

[KoTwist] E. Kowalski : *On the rank of quadratic twists of elliptic curves over function fields*, International J. of Number Theory 2 (2006), 267–288.

[KoSieve] E. Kowalski : *The large sieve and its applications*, Cambridge Tracts in Math. 175, Cambridge Univ. Press, and *The principle of the large sieve*, `arXiv:math.NT/0610021`

[KoZeta2] E. Kowalski: *The large sieve, monodromy and zeta functions of algebraic curves, II: Independence of the zeros*, IMRN, Vol. 2008.

[LaA]   S. Lang : *Algebra*, Revised 3rd Edition, GTM 211, Springer-Verlag (2002).

[R]   Rodriguez-Villegas, F.: *The bezoutian and hypergeometric functions*, unpublished note.

[SpSt] T. A. Springer and R. Steinberg : *Conjugacy classes*, Seminar on Algebraic Groups and Related Finite Groups, Lecture Notes in Mathematics, 131, (1968-69), 167-266, Springer-Verlag, Berlin-New York, 1970.

[Za]   H. Zassenhaus : *On the spinor norm*, Arch. Math. 13 (1962), 434–451.

Dept. of Mathematics, The University of Texas at Austin, 1 University Station C1200, Austin, TX, 78712, USA.

E-mail address: jouve@math.utexas.edu